BAB II

TINJAUAN PUSTAKA

2.1 Studi Literatur

Kasus pada penelitian ini bukan pertama kalinya, terdapat beberapa penelitian yang dapat dijadikan rujukan sehingga penulis dapat menjadikannya refrensi penelitan. Kasus pada penelitian sebelumnya merupakan kasus yang sama, hanya saja pada penelitian ini memberikan analisis dan pendeteksian dari serangan yang dilakukan. Berikut merupakan *literature review* dari penelitian terdahulu yang berkaitan dengan *live forensics*:

Tabel 2.1 *Literature Review*

No	Nama	Judul	Uraian Singkat	Hasil
1	(Nita Hildayanti, Imam Riadi, 2019)	*Forensics Analysis of Router On Computer Networks Using Live Forensics Method*	Penelitian ini menemukan data pada proses kerja Router menggunakan metode *forensics*, sehingga dapat membantu dalam memberikan informasi tentang penggunaan internet yang terserang *ARP Spoofing* dari pengguna lain (*attacker*).	Informasi yang didapatkan dari hasil simulasi serangan Netcut pada jaringan Router adalah IP meminta *request* pada DNS namun tidak ada respon sehingga permintaan terjadi terus menerus dari IP ke DNS kemudian *protocol* TCP akan ditampilkan secara terus menerus karena data yang dikirim oleh TCP ke penerima dianggap memiliki kesalahan.
2	(Dedy Saputra, Imam Riadi, 2019)	*Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method*	Penelitian ini menemukan bukti digital pada serangan *sniffing* dengan menggunakan metode *live forensics* dan Proses pendeteksian serangan menggunakan aplikasi IDS *Snort*.	Hasil dari pengujian penelitian ini mampu menyadap aktivitas dari pengguna jaringan sehingga dapat mengetahui *password* dan *user* saat melakukan *request login* pada *web server*, analisis *data log* ini dilakukan menggunakan *Wireshark*. sedangkan untuk mitigasinya dapat dilakukan menggunakan

3	(Muhammad Sabri Ahmad, Imam Riadi, Yudi Prayudi, 2017)	Investigasi *Live Forensics* Dari Sisi Pengguna Untuk Menganalisa Serangan *Man In The Middle Attack* Berbasis Evil Twin	Pada penelitian ini mendeteksi serangan MITM berbasis Evil Twin dengan menggunakan metode *live forensics* dengan pendekatan dari sisi *user*. Serangan tersebut dapat diketahui dengan cara menganalisa atribut dari AP tersebut.	Terdapat beberapa temuan yang dapat dijadikan informasi yaitu berupa IP Address, MAC Address pelaku dan beberapa *file* yang mencurigakan seperti *file html,css, jpg* dan *png*. Proses analisa hirarki, ditemukan dua objek yang dapat dianalisa lebih lanjut, karena memiliki tingkat presentasi aktivitas yang cukup tinggi yaitu *port* ARP dan *Port* HTTP. Dari hasil analisa filterisasi *port* HTTP ditemukan IP 10.0.0.20 melakukan *request* ke IP 104.28.18.80
4	(Muhammad Alim Zulkifli, 2018)	Metode *Live Forensics* untuk Analisis Serangan *Denial of Services* (DoS) pada Router	Pada penelitian ini dilakukakknnya analisis serangan DoS pada Router melalui data dari lalu lintas jaringan sehingga dapat menggali informasi serta menarik data forensik sebagai bukti digital dari serangan DoS pada Router melalu metode *live forensics*.	Penelitian ini berhasil menarik data informasi serangan DoS pada Router terkait data log aktivitas dan alamat IP penyerang melalui proses penelitian meliputi proses observasi pada Router, pengujian serangan DoS. Penelitian ini berhasil menemukan bukti digital dan karakteristik dari serangan DoS dengan menggunakan metode *live forensics*.

5	(Tobias Fiebig, 2013)	*Forensic DHCP Information Extraction from Home Routers*	Pada penelitian ini dilakukannya penggalian informasi dan menjelaskan tahapan observasi dalam melakukan ekstrak informasi dengan memanfaatkan JTAG pada Router kelas kecil atau yang biasanya dikenal dengan *Home Routers*.	Dapat menemukan informasi dari *hostname* serta MAC address dari perangkat pengguna yang terhubung pada jaringan dengan memanfaatkan *memory router*. Penerapan metode *live forensics* dapat mengumpulkan bukti digital yang terdapat pada SCADA (*Supervisory Control and Data Acquisition System*). Pengumpulan bukti digital didasarkan dari perubahan aktivitas dan *traffic* komunikasi yang abnormal.

Dari informasi pada Tabel 2.1 *literature review* di atas dapat diketahui jika metode *live forensics* merupakan metode yang dapat menganalisis sebuah data yang bersifat *data volatile* dan hanya bisa didapatkan pada saat sistem sedang menyala dan berjalan sehingga metode tersebut cocok untuk diterapkan pada kasus penelitian ini. Sedangkan pada informasi di bawah ini merupakan uraian singkat dari penelitian yang diusulkan penulis, seperti yang terlampir pada Tabel 2.2 berikut:

Tabel 2.2 Penelitian yang diusulkan

Judul	Uraian singkat	Solusi	Hasil yang diharapkan
Analisis *Address Resolution Protocol Poisoning Attack* pada Router WLAN Menggunakan Metode *Live Forensics*	Menganalisis dan mendeteksi serangan *ARP poisoning* sehingga dapat menemukan bukti digital dari serangan dan hasil deteksi pada Snort. Objek yang di analisis berupa *traffic* jaringan pada Router WLAN	Melakukan analisis serangan ARP *poisoning* menggunakan metode *live forensics* dengan memanfaatkan aplikasi *Wiresharks* sebagai alat untuk memonitoring	1. Mendapatkan informasi serangan dari hasil proses monitoring *traffic* jaringan pada perangkat Router. 2. Mengetahui dan mengidentifikasi karakteristik informasi yang berhubungan dengan serangan

	dikarenakan berbagai aktivitas jaringan dapat terdeteksi pada *traffic* jaringan yang ada pada Router. Hasil analisis dari informasi yang didapatkan pada *traffic* jaringan digunakan sebagai bukti digital sehingga nanti dapat memetakan jenis informasi dari hasil penelitian.	*traffic* jaringan. Sedangkan pendeteksian serangan *ARP poisoning* menggunakan aplikasi IDS *Snort* dengan memberikan *rules* pada *Snort* sehingga dapat mengirimkan *alert* jika terjadi sebuah serangan.	*ARP poisoning* dari paket-paket yang ada pada *traffic* jaringan. 3. Setelah menyimpulkan informasi dari paket yang teridentifikasi melakukan serangan maka dapat diketahui *variable*/komponen apa saja yang terdeteksi melewati perangkat Router sehingga informasi tersebut dapat dilampirkan pada laporan dari hasil penelitian ini.

2.2 Wireless Local Area Network (WLAN)

Wireless Local Area Network adalah jaringan *Local Area Network* yang menggunakan media frekuensi radio (RF) dan *infrared* (IR) [1]. Teknologi ini digunakan untuk menghubungkan penggunanya ke internet melalui perangkat Router dan untuk penggunanya sendiri sudah banyak ditemukan diberbagai kalangan, baik pada keluarga, badan usaha, kampus, maupun instansi kepemerintahan. Pemakaian yang sangat mudah dan efisien menjadikan teknologi WLAN ini sangat populer. Tetapi dibalik semua itu terdapat beberapa ancaman yang dapat merugikan pengguna, salah satunya yaitu serangan *Man In The Middle Attack* pada jaringan Router WLAN. Oleh karena itu setidaknya kita dapat memperhatikan kemanan informasi pada jaringan WLAN tersebut.

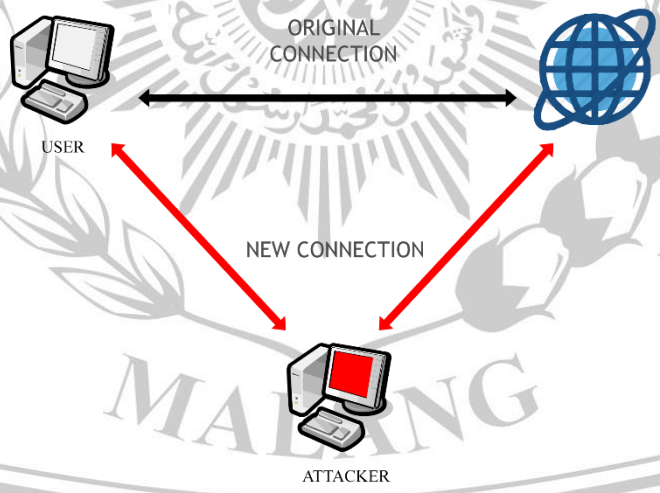
2.3 Router

Router merupakan suatu perangkat keras yang berada pada sebuah jaringan komputer yang mampu melewatkan paket IP dari suatu jaringan ke jaringan lainnya. Router juga dapat digunakan untuk menghubungkan LAN ke sebuah

layanan telekomunikasi. Pada dasarnya, fungsi dari Router yaitu untuk menghubungkan beberapa jaringan dan mengatur lalu lintas data. Selain itu Router dapat mengirimkan paket *data* dan mentransmisikan informasi *data* dari satu jaringan ke jaringan lainnya. Posisi dari Router ini terbilang sangat sensitif dan kritis di dalam sebuah jaringan karena dapat mencegat, memodifikasi lalu lintas, serta dapat bertindak sebagai *sniffer* dalam memonitor jaringan, sehingga hal tersebut membuat Router biasanya menjadi sasaran umum untuk dapat diserang [12].

2.4 ARP Poisoning

ARP Poisoning merupakan jenis serangan *Man In The Middle Attack* yang ada pada jaringan LAN ataupun WLAN dengan akses terbuka. Serangan ini mampu mengendus *frame data* dan melakukan modifikasi *traffic* atau bahkan menghentikan *traffic* [3] [4]. Konsep dasar dari serangan ini yaitu dengan memanfaatkan *ARP Cache* untuk memberikan identitas/alamat *server* atau *Gateaway* palsu kepada pengguna jaringan. Berikut merupakan tampilan dari cara kerja *ARP Poisoning*.



Gambar 2.1 *ARP Poisoning Attack*

Pada gambar 2.1 di atas diketahui bahwa *attacker* memberikan koneksi baru pada pengguna jaringan sehingga korban dari serangan tersebut berada pada koneksi palsu yang telah dialihkan oleh *attacker*, dengan begitu *attacker* tersebut dapat dengan mudah mencegat maupun memodifikasi *traffic data* pada jaringan tersebut. Jika dibiarkan, serangan tersebut dapat mengganggu lalu lintas jaringan

sehingga dapat memutuskan koneksi internet pada perangkat korban. Oleh karena itu dibutuhkan penelitian yang dapat mendeteksi perilaku dari serangan ARP Poisoning ini [6].

2.5 Kali Linux

Kali Linux atau biasa disebut dengan *BackTrack* adalah sistem operasi *open source* berbasis *debian linux* yang memiliki banyak keunikan pada bidang pengujian penetrasi, dengan berfokus pada tiga kolaborasi pengujian penetrasi yang beragam yaitu auditor, IWHAX, dan WHOPPIX [15]. Kali Linux diciptakan secara khusus untuk memenuhi keperluan dalam bidang *penetration testing* pada sebuah sebuah *system* beserta proses auditor keamananya. Terdapat lebih dari 300 *security tools* yang telah terintegrasi pada sistem operasi Kali Linux sehingga penggunaan sistem operasi ini sangat cocok dalam menyelesaikan kasus pada penelitian ini.

2.6 Netcut

Netcut adalah salah satu aplikasi yang digunakan untuk mengontrol dan memodifikasi *traffic data* akses jaringan *wireless*, dan memiliki fungsi lain yaitu sebagai pemotong akses *internet public* maupun *private* yang berada pada jaringan *local area network* [16]. Akan tetapi aplikasi *netcut* ini banyak disalah gunakan untuk tujuan tertentu seperti memutuskan jaringan terhadap pengguna yang lain agar bisa mendapatkan *bandwith internet* yang lebih besar. Serangan tersebut menggunakan konsep dari metode ARP Poisoning yang memberikan informasi *gateaway* palsu ke *target* serangan sehingga akan menjadikan dirinya sebagai *gateway* atau pintu sebelum mengakses *internet*. Berdasarkan pada konsep dari metode tersebut pemilihan *tools* ini digunakan sebagai langkah dalam melakukan pengujian serangan.

2.7 Digital Forensics

Digital forensics muncul sebagai suatu ilmu pengetahuan dan keahlian yang berkembang secara terus menerus dalam mengidentifikasi, mengoleksi, menganalisis serta menguji bukti-bukti digital [7]. Digital forensics Pada umumnya terdapat dua jenis analisis *digital forensics* yaitu *dead forensics* dan *live forensics* [8]. Dalam hal ini *digital forensics* berkaitan dengan pemantauan serta analisis pada lalu lintas jaringan komputer *local area network* yang bertujuan untuk

mengumpulkan informasi, bukti, dan mendeteksi adanya serangan. Penelitian ini mengambil metode analisis dari *digital forensics* yang bersifat *realtime*, dikarenakan perangkat yang diteliti adalah *traffic data* pada Router WLAN yang bersifat *data volatile* sehingga analisis secara *realtime* merupakan langkah yang tepat dalam menganalisis penelitian ini.

2.8 Live Forensics

Live forensics adalah teknik analisis yang melibatkan data-data yang berjalan pada sistem, seperti data yang terdapat pada RAM, Router, *network process*, *memory, swap file, running system process* sehingga dapat memberikan gambaran dari proses pada sistem yang berjalan [9] [10]. *Live analysis* merupakan cara terbaik untuk menyelidiki sistem target [11] yang selalu berjalan contohnya pada perangkat jaringan *wireless* seperti Router *memory*, sedangkan memory tersebut terbagi menjadi dua jenis, yaitu non-volatile dan volatile *memory* [17]. Router merupakan perangkat yang posisinya sangat penting pada suatu jaringan dikarenakan Router dapat mencegat, memodifikasi *traffic data* dan dapat bertindak sebagai *sniffer* dalam memonitoring jaringan, sehingga Router sering menjadi sasaran umum untuk dapat diserang. Oleh karena itu fokus penelitian analisis *live forensics* ini terdapat pada Router WLAN karena informasi yang terkandung pada Router berupa *data volatile* yang berhubungan dengan analisis *live forensics*. Pengambilan informasi tersebut dilakukan dengan cara memonitoring *traffic* jaringan pada Router dengan menggunakan aplikasi *Wireshark* yang memang dipergunakan untuk pemeriksaan keamanan jaringan serta mengatasi permasalahan jaringan [7].

2.9 IDS Snort

Intrusion Detection System (IDS) berbentuk *Snort* merupakan aplikasi yang bertujuan untuk melakukan pendeteksian serangan [16]. Snort bekerja dengan cara memantau berkas-berkas pada *operating system* dan jika terdapat sistem yang berjalan mencurigakan maka *Snort* dapat mendeteksi dan memunculkan *alert* pada penggunanya. Semua serangan yang terpantau oleh *Snort* akan tersimpan pada *log Snort*, sehingga penggunanya mampu memeriksa dan menganalsis setiap kegiatan yang telah berjalan pada *operating system* perangkatnya. Serangan dapat terpantau sesuai *rules* yang sebelumnya telah dikonfigurasi pada *file Snort*, sehingga

penggunanya dapat dengan mudah untuk mengkontrol dan menentukan jenis serangan apa saja yang dapat dibaca dan dideteksi oleh *Snort*.

2.10 Wireshark

Wireshark adalah apikasi yang dipergunakan untuk pemeriksaan keamanan jaringan serta mengatasi permasalahan jaringan [7]. Aplikasi ini dapat merekam semua paket yang lewat serta dapat menampilkan dan menyeleksi *data* tersebut dengan sedetail mungkin, contohnya data *username* dan *password* sekalipun dapat terbaca pada aplikasi ini. *Wireshark* banyak disukai dikarenakan tampilan yang didapatkan sudah berupa *Graphical User Interface* (GUI) atau biasa disebut tampilan grafis. Hal ini tentunya mempermudah penggunanya dalam menggunakan aplikasi tersebut. Dalam penggunaannya *Wireshark* juga digunakan sebagai tahapan dalam mengetahui karakteristik dari informasi serangan sehingga dapat menemukan bukti digital pada sebuah kasus yang ada di dalam sebuah jaringan.